CFO 1750205/Sun

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　７月　２日

出願番号
Application Number: 特願２００３－１８９９２４

[ST. 10/C]: [ＪＰ２００３－１８９９２４]

出願人
Applicant(s): キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００３年　９月１６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

BEST AVAILABLE COPY

出証番号　出証特２００３－３０７５６９０

【書類名】　特許願
【整理番号】　255274
【提出日】　平成15年 7月 2日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 13/00
【発明の名称】　サーバ装置
【請求項の数】　18
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　明星　俊彦
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　山嵜　信一
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100087446
【弁理士】
【氏名又は名称】　川久保　新一
【先の出願に基づく優先権主張】
【出願番号】　特願2002-247899
【出願日】　平成14年 8月28日
【手数料の表示】
【予納台帳番号】　009634
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704186

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　サーバ装置

【特許請求の範囲】

【請求項１】　会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、

認証手続きを行う際に用いる認証情報に基づいて、上記参加者の立場を判別する参加者判別手段を有することを特徴とするサーバ装置。

【請求項２】　請求項１において、

上記複数の電子機器は、Ｂｌｕｅｔｏｏｔｈによって上記アクセスポイントと接続され、

上記参加者判別手段は、上記電子機器とアクセスポイントとの間の認証に用いたＰＩＮコードに基づいて、上記参加者の立場を判別することを特徴とするサーバ装置。

【請求項３】　請求項１または請求項２において、

上記参加者判別手段は、会議の主催者と上記主催者以外の参加者とを判別する手段であり、

上記会議システムの管理サーバは、上記主催者と上記参加者との操作制限を行う操作制限テーブルを有することを特徴とするサーバ装置。

【請求項４】　請求項３において、

上記操作制限テーブルで制限される項目は、他のネットワークへの接続制限の項目を含む項目であることを特徴とするサーバ装置。

【請求項５】　請求項４において、

上記電子機器に、ＩＰアドレスを割り当てると同時に、ＩＰアドレステーブルを作成するＩＰアドレステーブル作成部を有することを特徴とするサーバ装置。

【請求項６】　請求項５において、

上記ＩＰアドレステーブル作成部が作成したＩＰアドレステーブルと、ネット

ワークに接続されたゲートウェイが持つＩＰアドレステーブルとを、共有して記憶するＩＰアドレス記憶部を有することを特徴とするサーバ装置。

【請求項７】　会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、

認証手続きを行う際に用いる認証情報に基づいて、上記認証手続を行った電子機器に、上記通信システムにおける機能制限を割り当てることを特徴とするサーバ装置。

【請求項８】　会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、

認証手続きを行う際に用いる認証情報に基づいて、上記認証手続を行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする通信システム。

【請求項９】　会議に参加するユーザによって操作される複数の電子機器と、上記電子機器との間で情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される通信システムのサーバ装置において、

認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記参加者の立場を判別する参加者判別手段を有することを特徴とするサーバ装置。

【請求項１０】　請求項９において、

上記認証手続きは、無線リンクプロトコルレベルによる認証とリンクレベルよりも高いプロトコルレベルによる認証によって構成される手続であることを特徴とするサーバ装置。

【請求項１１】　請求項１０において、

上記認証手続きにおいて、無線リンクレベルによる認証では、リンク確立時にＢｌｕｅｔｏｏｔｈにおけるＰＩＮコードを照会して認証を行い、上位プロトコルレベルによる認証では、上記無線リンクレベルでの認証動作を省くことを特徴とするサーバ装置。

【請求項１２】　請求項９において、

上記認証手続きは、認証のプロトコルレベルに応じて、異なる手順によって認証操作を行わせ、この認証手順の方法に基づいて、参加者の立場を判別することを特徴とするサーバ装置。

【請求項１３】　請求項９において、

上記参加者判別手段は、会議の主催者と、他のネットワークへのアクセス権限を持たずしかも上記会議の主催者以外の参加者と、他のネットワークへのアクセス権限を持ちしかも上記会議の主催者以外の参加者とを判別する手段であることを特徴とするサーバ装置。

【請求項１４】　請求項１３において、

上記参加者判別手段による判別に基づいて、電子機器へのＩＰアドレスの割り当てを行うことを特徴とするサーバ装置。

【請求項１５】　会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、

認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記認証手続を行った電子機器に、上記会議システムにおける機能制限を割り当てることを特徴とするサーバ装置。

【請求項１６】　請求項１５において、

上記認証情報は、ＢｌｕｅｔｏｏｔｈにおけるＰＩＮコードと、上位プロトコルとの認証で定められた認証情報であることを特徴とするサーバ装置。

【請求項１７】　会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおいて、

認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記認証手続を行った電子機器に、上記会議システムにおける機能制限を割り当てることを特徴とする通信システム。

【請求項１８】　アクセスポイントを有する通信システムのサーバ装置において、

上記アクセスポイントが無線通信機器を認証する際に用いた認証情報に基づいて、上記無線通信機器の上記通信システム内の機能制限を行うことを特徴とするサーバ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信システム、通信装置に係り、たとえば、会議システムを用いた会議の参加者の立場の判断と、会議システムにおける機能制限の割り当てとに関する。

【０００２】

【従来の技術】

従来の会議では、紙ベースで発表資料を参加者全員に配布するので、資源が無駄であるという欠点がある。また、資料が人数分揃わない場合には、不足部数を慌ててコピーし、会議の進行を妨げるという欠点がある。

【０００３】

一方、近年は、発表者が、ＰＣ（パーソナルコンピュータ）やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）を、会議室に持ち込み、発表資料をプロジェクタで投影し、プレゼンテーションすることが一般である。さらに、発表者以外の参加者にも、紙ベースではなく、ネットワーク経由で、資料データを配布することによって、上記欠点を克服している。

【０００４】

しかし、参加者が多い会議で、全員がネットワークを使用すると、配線が複雑になるという新たな欠点が生じる。この新たな欠点を克服するために、Ｂｌｕｅｔｏｏｔｈ等の無線通信を用いた会議システムが考えられている。

【０００５】

Ｂｌｕｅｔｏｏｔｈ方式は、アドホックなマルチポイント接続を行うので、最大接続数が、８機器、通信範囲が１０ｍのピコネットを構築し、通信することが

でき、通信速度に関しては、非同期通信において、下り７２１Ｋｂｐｓ、上り５７．６Ｋｂｐｓの通信を行うことができる。また、音声通信もサポートし、１つのチャネルで、音声とデータとを転送することができる等、多種多様なプラットフォームでの利用が期待されている。

【０００６】

上記Ｂｌｕｅｔｏｏｔｈ等の無線通信を用いた会議システムによって、配線の煩雑さは解消されるが、無線接続による外部からの不正アクセス、データの改ざん等セキュリティ面で、別の欠点が浮上している。

【０００７】

しかも、一度認証を通ると、資料のコピー、プリントアウト、データの上書き等については、Ｂｌｕｅｔｏｏｔｈの認証レベルでは制限することができないという別の欠点がある。

【０００８】

上記別の欠点を克服するために、プライベート用のＰＩＮコードとテンポラリ用のＰＩＮコードとの２種類のＰＩＮコードを、機器の利用形態によって使分けることによって、利便性とセキュリティレベルとを向上する方法が提案されている（たとえば、特許文献１参照）。また、会議中の権限を、各端末に指定し、機能を制限することが提案されている（たとえば、特許文献２参照）。

【０００９】

また、上記不正アクセス、データの改ざんの問題やアクセス制御の問題に対して、Ｐｏｒｔ　Ｂａｓｅｄ　Ｎｅｔｗｏｒｋ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ技術によってセキュリティ強化を目的とした標準か作業が進んでいる（たとえば、非特許文献１参照）。

【００１０】

【特許文献１】

特開２００１－３１２４７２号公報

【特許文献２】

特開２００１－３３１４３１号公報

【非特許文献１】

ＩＥＥＥ８０２．１ｘ（Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｅｌｅｃｔｒｉｃａｌ　ａｎｄ　Ｅｌｅｃｔｒｏｎｉｃ　Ｅｎｇｉｎｅｅｒｓ　８０２．１ｘ）

【００１１】

【発明が解決しようとする課題】

特許文献２記載の発明では、参加者の機器に権限を与える際に、会議システムのアプリケーション上から、各参加者がどの権限で会議に参加するかを特定するタブを選択し、選択したタブに応じた権限を設定する。

【００１２】

しかし、このようにすると、参加者の手間がかかる上、任意に権限の設定を変更することができ、権限を故意に変えてデータを操作することも可能であるという問題がある。

【００１３】

一方、非特許文献１記載の発明では、端末認証サーバとしてＲＡＤＩＵＳ（Ｒｅｍｏｔｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｄｉａｌ－Ｉｎ　Ｕｓｅｒ　Ｓｅｒｖｉｃｅ）サーバを設置し、端末が会議システムへアクセスするに先立って、認証サーバとの間で電子証明書やパスワード等を用いて認証を行う方法をとっている。

【００１４】

しかし、このような構成では、会議参加者は、ＩＥＥＥ８０２．１ｘに対応したプログラムを有する端末のみでしか、会議に参加することができず、ＩＥＥＥ８０２．１ｘが検討される以前の端末や、Ｂｌｕｅｔｏｏｔｈが多く実装されているＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｃｅ）等で、ＩＥＥＥ８０２．１ｘに対応していない機器を持ち込んで会議に参加することができないという問題がある。

【００１５】

本発明は、会議システム等のシステムに接続する機器によるデータの不正な改ざんや情報の漏洩を防ぐことができ、しかも、機能制限をアプリケーション上で別個に行う手間を省くことができる通信システムのサーバ装置を提供することを

目的とするものである。

【００１６】

【課題を解決するための手段】

本発明は、会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、認証手続きを行う際に用いる認証情報に基づいて、上記参加者の立場を判別する参加者判別手段を有することを特徴とするサーバ装置である。

【００１７】

また、本発明は、会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、認証手続きを行う際に用いる認証情報に基づいて、上記認証手続を行った電子機器に、上記通信システムにおける機能制限を割り当てることを特徴とするサーバ装置である。

【００１８】

さらに、本発明は、会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、認証手続きを行う際に用いる認証情報に基づいて、上記認証手続を行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする通信システムである。

【００１９】

そして、本発明は、会議に参加するユーザによって操作される複数の電子機器と、上記電子機器との間で情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される通信システムのサーバ装置において、認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記参加者の立場を判別する参加者判別手段を有することを特徴とするサーバ装

置である。

【００２０】

また、本発明は、会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記認証手続を行った電子機器に、上記会議システムにおける機能制限を割り当てることを特徴とするサーバ装置である。

【００２１】

さらに、本発明は、会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおいて、認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記認証手続を行った電子機器に、上記会議システムにおける機能制限を割り当てることを特徴とする通信システムである。

【００２２】

そして、本発明は、アクセスポイントを有する通信システムのサーバ装置において、上記アクセスポイントが無線通信機器を認証する際に用いた認証情報に基づいて、上記無線通信機器の上記通信システム内の機能制限を行うことを特徴とするサーバ装置である。

【００２３】

【発明の実施の形態および実施例】

［第１の実施例］

図１は、本発明の第１の実施例である無線通信システムＷＣ１を示すブロック図である。

【００２４】

無線通信システムＷＣ１は、会議システム管理サーバ１０と、アクセスポイント２０と、ゲートウェイ３０と、ＰＣ４０と、ＬＡＮ５０と、広域ネットワーク

６０を有する。

【００２５】

会議システム管理サーバ１０は、広域ネットワーク６０へアクセスするために必要であり、会議システムのアプリケーションを動作させるサーバである。

【００２６】

ＰＣ４０は、会議主催者や参加者が持参した無線端末の例であり、Ｂｌｕｅｔｏｏｔｈによる無線接続が可能である。

【００２７】

アクセスポイント２０は、無線端末としてのＰＣ４０から、根幹のＬＡＮ５０に接続する際に必要となるポイントである。また、アクセスポイント２０は、根幹のＬＡＮ５０に接続され、一般的なスイッチングハブのような役目をする。会議主催者や参加者が持参したＰＣ４０を有線で会議サーバ１０に接続する場合、ハブを用いて、会議システム管理サーバ１０に複数台接続することができるが、無線接続する場合は、各機器をアクセスポイント２０に接続し、アクセスポイント２０経由で、会議システム管理サーバ１０との間で、データをやりとりする。

【００２８】

アクセスポイント２０へ接続する場合、セキュリティを考慮し、ユーザ認証する必要がある。一般的に、ＰＩＮコード（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を、機器間で交換することによって、ユーザ認証するが、アクセスポイント２０のデフォルトＰＩＮコードが固定であると、一度接続したことのある人なら、同じＰＩＮコードを使って何度でも接続でき、セキュリティ面で問題がある。

【００２９】

そこで、本実施例では会議の主催者が、デフォルトＰＩＮコードで、アクセスポイント２０に予め接続し、会議の時にのみ有効なＰＩＮコードに変更する方法を採る。この場合、デフォルトＰＩＮコードが固定であると、上記のように、誰でも設定を変更できるので、デフォルトＰＩＮコードを故意に変更することもできる。すると、正規の主催者が、会議の時にのみ有効なＰＩＮコードに変更しようと考え、デフォルトＰＩＮコードで接続しようとしても、接続できないという

事態が生じる。

【００３０】

そこで、会議システム管理サーバ１０によって運営される会議室予約システム等で会議室を予約した時に、その会議室付属のアクセスポイント２０にデフォルトＰＩＮコードが設定され、同時に、主催者にメール等で通知し、主催者は、会議システム管理サーバ１０から通知されたＰＩＮコードを使ってアクセスポイント２０に接続し、会議の時にのみ有効なＰＩＮコードに変更する手段がとられている。参加者は、主催者から予め通知された会議の時にのみ有効なＰＩＮコードを含む参加証を持って、会議室に臨み接続する。

【００３１】

図２は、本実施例における会議システム管理サーバ１０を示すブロック図である。

【００３２】

会議システム管理サーバ１０は、主制御部（ＣＰＵ）１２と、ネットワーク通信部１３と、記憶部１４と、データベース１５と、入力部１６と、表示部１７と、テーブル作成部１８と、判別部１９とを有する。

【００３３】

主制御部１２は、会議システム制御、各種アプリケーションの管理、入力部、表示部を制御する。

【００３４】

ネットワーク通信部１３は、主制御部１２の指示に従って、有線通信網、無線通信網に接続される各種無線端末としてのＰＣ４０との間で、データを送受信する。記憶部１４は、テーブル作成部１８で作成された各種テーブルデータやファイル管理を行う。

【００３５】

入力部１６は、キーボード、マウス等によって入力を制御し、表示部１７は、ＣＲＴモニタ等の表示を制御する。テーブル作成部１８は、ＩＰアドレステーブルや機能制限テーブル等各種テーブルを作成する。判別部１９は、ネットワーク通信部１３が取得した参加証に基づいて、その参加証の送り主が会議の主催者で

あるか、参加者であるかを判別する。

【００３６】

図３は、本実施例において、会議の主催者が会議に参加するまでの動作を示すフローチャートである。

【００３７】

まず、会議の主催者は、会議室予約システム等で会議室を予約し（Ｓ１）、アクセスポイント２０に設定されているデフォルトＰＩＮコードを使って、アクセスポイント２０に接続し、会議の時にのみ有効なＰＩＮコードに設定を変更する（Ｓ２）。そして、その会議の時にのみ有効なＰＩＮコードを、会議の参加者に電子メール等で通知する（Ｓ３）。

【００３８】

次に、メールアドレス、ＰＩＮコード、社員ＩＤ等が記されている主催者用の参加証ファイルと、主催者以外の会議参加者用の参加証ファイルとを作成し（Ｓ４）、この作成したファイルを、参加者全員にそれぞれ電子メール等で配布し（Ｓ５）、会議に参加する（Ｓ６）。なお、主催者用の参加証には、デフォルトＰＩＮコードと、会議の時にのみ有効なＰＩＮコードとの２つのコードが記述され、主催者以外の会議参加者の参加証には、会議の時にのみ有効なＰＩＮコードのみが記述され、主催者以外の参加者には、主催者以外の会議参加者用の参加証ファイルを配布する。

【００３９】

図４は、本実施例において、会議の参加者が会議に参加するまでの動作を示すフローチャートである。

【００４０】

まず、主催者が配布した会議の時にのみ有効なＰＩＮコードを、参加者が取得する（Ｓ１１）。このＰＩＮコードの取得方法は、電子メールのみでなく、主催者が作成したＷｅｂ等にアクセスし、主催者が配布した会議の時にのみ有効なＰＩＮコードを取得するようにしてもよい。

【００４１】

次に、主催者が配布した参加証を、参加者が受け取り（Ｓ１２）、参加者はそ

の参加証を持参し、会議に参加する（Ｓ１３）。この参加証には、ＰＩＮコードが記載されているので、会議の時にのみ有効なＰＩＮコードを取得する処理（Ｓ１１）を省くようにしてもよい。

【００４２】

図５は、本実施例において、主催者がアクセスポイント２０のＰＩＮコードを変更する処理を示すシーケンス図である。

【００４３】

まず、主催者が会議室予約システムで会議室の予約を行うと、会議システム管理サーバ１０は、ＬＡＮ５０経由でアクセスポイント２０に接続し、アクセスポイント２０に、デフォルトＰＩＮコードを設定する（Ｓ２１）。この会議システム管理サーバ１０は、会議室予約システムを運用し、会議室予約システムで会議室の予約が行われた際に、自動的にＰＩＮコードを作成し、このＰＩＮコードをデフォルトＰＩＮコードとしてアクセスポイント２０に設定し、同時に、このデフォルトＰＩＮコードを予約者に通知するような機能を有する。

【００４４】

主催者は、会議システム管理サーバ１０からデフォルトＰＩＮコードの通知を受けると、このデフォルトＰＩＮコードと、会議の際に使用する会議の時にのみ有効なＰＩＮコードとを、無線機器としてのＰＣ４０に設定する。

【００４５】

次に、主催者は、所有の無線機器としてのＰＣ４０から、アクセスポイント２０に、接続要求を発行する（Ｓ２２）。アクセスポイント２０は、接続要求を受け、データが正しければ、接続確立のメッセージを、主催者のＰＣ４０に送信し、接続が確立する（Ｓ２３）。

【００４６】

その後に、アクセスポイント２０は、主催者のＰＣ４０に認証要求を発行し、パスワードの要求を促す（Ｓ２４）。主催者側のＰＣ４０は、認証要求を受けると、予め設定しておいたデフォルトＰＩＮコードを、アクセスポイント２０に送信する（Ｓ２５）。アクセスポイント２０は、主催者のＰＣ４０から送られたＰＩＮコードが正しければ、主催者のＰＣ４０に認証完了を通知する（Ｓ２６）。

【００４７】

次に、主催者のＰＣ４０は、ＰＩＮコードの設定変更要求を、アクセスポイント２０に発行し（Ｓ２７）、これを受けたアクセスポイント２０から、要求メッセージ受信応答が帰ってきたら（Ｓ２８）、予め設定しておいた会議の時にのみ有効なＰＩＮコードを送信する（Ｓ２９）。アクセスポイント２０は、新たなＰＩＮコードを受信すると、そのＰＩＮコードに設定を変更し、変更完了のメッセージを、主催者の無線機器としてのＰＣ４０に送信し、接続処理が完了する（Ｓ３０）。

【００４８】

なお、上記説明では、主催者のＰＣ４０からアクセスポイント２０に送信するデフォルトＰＩＮコードと、会議の時にのみ有効なＰＩＮコードとは、自動的に送信されるが、アクセスポイント２０からの要求に応じて、その都度、主催者が入力部（図示せず）を操作して入力し、上記入力されたＰＩＮコードを送信するようにしてもよい。

【００４９】

図６は、本実施例において、参加者が会議に参加する場合の処理を示すシーケンス図である。

【００５０】

なお、主催者が、図５で説明したＰＩＮコードの設定を変更した後に、一度、アクセスポイント２０との無線接続を切断し、再度、アクセスポイント２０に接続する場合も、上記と同様の処理を行う。

【００５１】

参加者は、主催者から通知された会議の時にのみ有効なＰＩＮコードを予めＰＣ４０に設定する。そして、会議室に着くと、所有のＰＣ４０から、アクセスポイント２０に、接続要求を発行する（Ｓ４１）。アクセスポイント２０は、接続要求を受け、データが正しければ、接続確立のメッセージを、参加者のＰＣ４０に送信し、接続が確立する（Ｓ４２）。

【００５２】

その後に、アクセスポイント２０が、参加者のＰＣ４０に認証要求を発行し、

パスワードの要求を促す（Ｓ４３）。参加者のＰＣ４０は、認証要求を受けると、予め設定しておいた会議の時にのみ有効なＰＩＮコードを送信する（Ｓ４４）。アクセスポイント２０は、参加者のＰＣ４０から送られてきたＰＩＮコードが正しければ認証完了のメッセージを送るので、参加者のＰＣ４０は、アクセスポイント２０から認証完了のメッセージを受信したら（Ｓ４５）、アクセスポイント２０を経由し、予め配布された参加証を、会議システム管理サーバ１０に送信する（Ｓ４６）。会議システム管理サーバ１０は、参加証を受信したら、図７で説明するような動作を行い、受信応答を参加者のＰＣ４０に送信し、接続処理が完了する（Ｓ４７）。

【００５３】

図７は、本実施例において、主催者または参加者から送られた参加証を受信した際に、会議システム管理サーバの判別部１９の動作を示すフローチャートである。

【００５４】

参加証には、最低限、ＰＩＮコードが記述されていることを前提とする。

【００５５】

会議システム管理サーバ１０は、図６のステップＳ４６で送信された参加証を受信すると、その参加証に記述されているＰＩＮコードを確認する。参加証に記述されているＰＩＮコードが２種類（デフォルトＰＩＮコード、会議の時にのみ有効なＰＩＮコード）であり（Ｓ５１）、しかも、会議システム管理サーバ１０が保持しているＰＩＮコードと一致すれば（Ｓ５３）、接続相手を主催者と判別し、その参加証を送信したＰＣ４０に、主催者としての機能権限を与える（Ｓ５６）。

【００５６】

一方、ＰＩＮコードが１種類（会議の時にのみ有効なＰＩＮコード）であり（Ｓ５１）、しかも、会議システム管理サーバ１０が保持しているＰＩＮコードと一致すれば（Ｓ５２）、主催者以外の参加者であると判別し、その参加証を送ってきたＰＣ４０に、主催者以外の参加者としての機能権限を与える（Ｓ５４）。不正なＰＩＮコードが記述された参加証を受信すれば、不正なアクセスとみなし

、そのＰＣ４０による全ての操作を不能にする（Ｓ５５）。

【００５７】

なお、上記説明では、接続完了後にＰＩＮコードが記述された参加証を転送する手順について記載したが、デフォルトＰＩＮコードを有しない参加者端末においては、接続時に、会議のときにのみ有効なＰＩＮコードを用いて接続するので、認証完了メッセージを受信した後の参加証転送を省くようにしてもよい。この場合、会議システム管理サーバ１０では、この参加証を受信したときにのみ、接続相手を判定し、正しく２種類のＰＩＮコードを有している場合には、主催者としての機能権限を与える制御を行い、それ以外の場合には、参加者としての機能権限を与えるようにアクセス制御を行い、これによって、上記説明と同様の機能を実現し、さらに参加証転送手順を省くことができる。

【００５８】

図８は、上記実施例において、会議システムによって制限される機能のテーブルを示す図である。

【００５９】

図７のステップＳ５６で主催者としての機能権限を与えられた場合は、図８に示す主催者の欄に丸印が記載されている機能を利用することができ、ステップＳ５４で主催者以外の参加者としての権限が与えられた場合は、参加者の欄に丸印が記載されている機能を利用することができ、バツ印が記載されている機能を利用することができない。なお、三角印は、制限付きでその機能を利用できることを示す。

【００６０】

ここで、図８に示す機能欄に記載されている「ファイルの閲覧」、「ファイルのコピー」、「ファイルの削除」、「ファイルの印刷」、「ファイル名変更」、「ファイルの上書き」は、図１に示すＬＡＮ５０経由で他の機器に公開されているファイルを、それぞれ、閲覧、コピー、削除、印刷、名称変更、上書きすることである。

【００６１】

「ファイルの保存」は、図１に示すＬＡＮ５０経由で接続されるサーバ等の機

器（たとえば、会議システム管理サーバ１０）にファイルを保存することである。「ネット閲覧」は、図１に示すゲートウェイ３０を介して，広域ネットワーク６０（インターネットやイントラネット）にアクセスする機能である。

【００６２】

「ＩＰアドレスの変更」は、アクセスポイント２０に接続し、会議システム管理サーバ１０から会議時の権限を与えられた際に、会議システム管理サーバ１０が割り当てたＩＰアドレスを変更する機能である。「ＰＩＮコードの変更」は、アクセスポイント２０に設定されているＰＩＮコード（会議の時にのみ有効なＰＩＮコード）を変更する機能である。「メールの送受信」は、ゲートウェイ３０を介して行う広域ネットワーク６０とのメールの送受信機能である。

【００６３】

［第２の実施例］

参加者それぞれに、外部アクセス可能なＩＰアドレスを割り当て、制限無しに広域ネットワーク６０へアクセスすることができると、参加者がＷｅｂのメールサービス等で重要な情報を、故意に外部に漏らす可能性がある。

【００６４】

そこで、本発明の第２の実施例は、第１の実施例の会議システム管理サーバ１０が、ＰＣ４０にＩＰアドレスを割り当てる方法を改良した実施例である。

【００６５】

つまり、第２の実施例は、図６のステップＳ４６で送信された参加証を受信した参加証に記述されているＰＩＮコードによって、会議システム管理サーバ１０が、広域ネットワーク６０へのアクセス制限をかける実施例である。

【００６６】

具体的には、図７のステップＳ５１において、ＰＩＮコードが、２種類（デフォルトＰＩＮコード、会議の時にのみ有効なＰＩＮコード）であり、しかも、会議システムが記憶し、保持しているデフォルトＰＩＮコードが、会議の時にのみ有効なＰＩＮコードと一致すれば（Ｓ５３）、その参加証を送信したＰＣ４０のユーザを主催者であると判別し、そのＰＣ４０の会議時の権限を、主催者として設定し、また、広域ネットワーク６０へ接続できるＩＰアドレスを、そのＰＣ４

０に割り当てる（Ｓ５６）。

【００６７】

ＰＩＮコードが、１種類（会議の時にのみ有効なＰＩＮコード）であり、しかも、正しいＰＩＮコードであれば（Ｓ５１、Ｓ５２）、その参加証を送信したＰＣ４０のユーザを、主催者以外の参加者であると判別し、そのＰＣ４０の会議時の権限を、主催者以外の参加者として設定し、また、広域ネットワーク６０へ接続できないＩＰアドレスを割り当てる。会議システム管理サーバ１０のＩＰアドレスを取得する場合、ＬＡＮ５０に接続されているゲートウェイ３０が持つＩＰアドレステーブルを取得し、共有することによって、会議システム管理サーバ１０のＩＰアドレスを取得する。

【００６８】

具体的には、無線端末としてのＰＣ４０が、会議システム管理サーバ１０に接続されたときに、会議システム管理サーバ１０は、ゲートウェイ３０が持つＩＰアドレステーブルを取得する。これと同時に、会議システム管理サーバ１０が取得する参加証に記載されているＰＩＮコードに基づいて、主催者であるか、参加者であるかを判別し、広域ネットワーク６０へのアクセスを許可できる無線端末に対して、ＩＰアドレスを配布する。

【００６９】

今回は、ゲートウェイ３０が持つＩＰアドレステーブルの取得を、無線端末の接続と同時に行ったが、一定時間間隔でテーブルを取得するようにしてもよい。

【００７０】

また、取得したＩＰアドレステーブルに、そのＩＰアドレスを追加し、ゲートウェイ３０に送信することによって、ゲートウェイ３０と会議システム管理サーバ１０とが、ＩＰアドレステーブルを共有する。

【００７１】

第２の実施例によれば、主催者と参加者とで、広域ネットワーク６０へのアクセス制限をかけることによって、不正な外部アクセスを防ぐことができる。

【００７２】

［第３の実施例］

会議システム管理サーバ１０では、参加者に与えるアクセス権限を、各無線端末としてのＰＣ４０から入力されるＰＩＮコードに基づいて判定し、それぞれにＩＰアドレスを割り当てる。しかし、この場合、ＩＥＥＥ８０２．１ｘのような上位プロトコルによる認証手順に対応している無線端末を有する参加者も、上位認証手順を使用することなく、無線リンクレベルでの認証を行う必要があり、機器のリソースを有効活用することができない。また、上位認証機能を会議システム管理サーバ１０に持たせた場合、同参加者は、上位認証手順に加え、ＰＩＮコードによる認証も必要になり、煩雑な操作を強いることになる。

【００７３】

本発明の第３の実施例は、会議システム管理サーバ１０に、ＩＥＥＥ８０２．１ｘ等の上位プロトコルによる認証機能を持たせ、同認証手順対応の無線端末による会議参加者と、非対応無線端末による会議参加者とが混在する場合に、各ＰＣ４０に有効な認証処理を行うアクセス制御に関する実施例である。

【００７４】

具体的には、第３の実施例は、上記会議システム管理サーバ１０に、上位認証機能（本実施例ではＩＥＥＥ８０２．１ｘとする）を持たせ、アクセスポイント２０において、ＰＩＮコードを要求するリンクレベルによる認証機能と、ＰＩＮコード入力を要求せずに無線端末との間におけるリンクレベルでの接続を許可し、リンクが確立した後に、上位認証手順を実行させる機能を持たせ、各認証結果に基づいて、アクセス権限を決定し、各無線端末としてのＰＣ４０に、ＩＰアドレスを割り当てる。

【００７５】

図９は、本発明の第３の実施例における各無線端末の操作と、その操作に従った会議システム管理サーバ１０の動作を示すフローチャートである。

【００７６】

はじめに、会議システム管理サーバ１０が運営する会議システムを、主催者が起動し（Ｓ６１）、アクセスポイント２０へリンク接続操作を行う。このログイン操作において、上記第１、２の実施例と同様に、デフォルト設定されているＰＩＮコードを用いて、リンクレベルの認証を行うと、会議システム管理サーバ１

０が、ログイン端末を、主催者のＰＣ４０であると判断し、主催者権限によるアクセス権を与えるＩＰアドレスを、同ＰＣ４０に割り当てる（Ｓ６２）。

【００７７】

ＩＰアドレスの割り当てを受け、ログイン動作が完了すると、次に、主催者は、会議の時のみ有効なＰＩＮコードの設定を行うために、ＰＩＮコード設定変更要求を発行し、アクセスポイント２０から要求に対する受信応答を受信すると、会議期間のみ有効となるＰＩＮコードを送信する。この新たなＰＩＮコードを受信したアクセスポイント２０は、受信したＰＩＮコードに設定変更を行い、変更完了メッセージを、主催者のＰＣ４０へ通知する（Ｓ６３）。

【００７８】

主催者のＰＣ４０は、ＰＩＮコードの設定変更が完了すると、ＰＩＮコードを要求するリンクレベルによる認証の際の使用するＰＩＮコードと、アクセスポイント２０と無線端末としてのＰＣ４０との間におけるリンクを確立した後に行う上位認証手順の際に、電子証明書を持っていないＰＣ４０が使用するアカウントとパスワードとが記されている参加証を作成し、参加者に配布する。

【００７９】

また、主催者は、機器操作によって会議システム管理サーバ１０へアクセスを行い、今回の会議で使用するアクセスポイント２０の名称、ミーティングＩＤ等の会議参加に必要となる情報を通知し、会議で使用する共有ディスプレイ（図示せず）の画面に、それらを表示するように依頼する（Ｓ６４）。会議システム管理サーバ１０は、上記依頼を受けると、会議で使用する共有ディスプレイの画面に、主催者から通知された上記情報を表示し、会議開催の準備を完了する。

【００８０】

一方、主催者以外の会議参加者は、会議が行われる場所で、クライアント端末を起動し（Ｓ６５）、先にディスプレイによって表示されているアクセスポイント２０の名称から、所望のアクセスポイント２０を選択し、アクセスポイント２０へ、接続要求信号を発行する。

【００８１】

ここで、参加者が選択するアクセスポイント２０は、参加者が持ち込んだ無線

端末の機能によって異なり、たとえば無線端末に、ＩＥＥＥ８０２．１ｘ等の上位認証手順処理（本実施例では上位認証手順としてＩＥＥＥ８０２．１ｘを実装した場合について記載し、以下は、８０２．１ｘサプリカント：Ｓｕｐｐｌｉｃａｎｔと記載）機能を有する場合、上位認証を行うために、リンク接続時にＰＩＮコード入力を要求しない設定のアクセスポイント２０を選択し、無線端末が８０２．１ｘサプリカント機能を持たない場合、リンク接続時にリンクレベルでの認証を行うアクセスポイント２０を選択する（Ｓ６６）。

【００８２】

ここで、８０２．１ｘサプリカント機能を持たない参加者端末が、リンクレベル認証が設定されているアクセスポイント２０へ接続要求を行うと、アクセスポイント２０から、リンクレベルでの認証を行うためのＰＩＮコード要求を受信する。

【００８３】

そして、参加者端末は、参加証によって通知されているＰＩＮコードを送信し、リンクレベル認証が確立されると（Ｓ６７）、会議システム管理サーバ１０は、参加者端末の認証ルートを判定し、この参加者用に設定されたＰＩＮコードによる接続であると判断すると（Ｓ７０）、会議参加者に与えられるアクセス制限をかけるＩＰアドレスを、参加者端末に割り当てる（Ｓ７１）。

【００８４】

また、８０２．１ｘサプリカント機能を有した端末が、上位認証設定されているアクセスポイント２０に、リンク接続要求を発行すると、参加者端末とアクセスポイント２０との間で、無線リンクが確立される。

【００８５】

そして、リンクが確立されると、参加者端末は、アクセスポイント２０の上位認証手順処理（ここでは、上記理由によって以下８０２．１ｘオーセンティケータ：Ａｕｔｈｅｎｔｉｃａｔｏｒと記載）機能に対して、認証要求を出力し、これを受けたアクセスポイント２０は、認証に必要なＩＤを要求し、その後に、ＩＥＥＥ８０２．１ｘ手順に従って、会議システム管理サーバ１０の認証サーバ機能との間で認証動作を行う（Ｓ６８）。

【００８６】

この時に、参加者端末が電子証明書を持っていれば、会議システム管理サーバ１０の認証サーバ機能によって認証され、仮に電子証明書を持っていなければ、会議システム管理サーバ１０の認証サーバ機能からアカウント名とパスワードとの要求が発行される。

【００８７】

これを受けた参加者端末では、参加証に含まれるアカウント名とパスワードとによって、認証手順を継続させ、会議への参加認証を受ける（Ｓ６９）。また、これらアカウントとパスワードとを入力したときに、他のネットワーク（たとえばイントラネットやインターネット）に接続するためのアカウントとパスワードとを、参加者が持っていれば、これら正規アカウント、パスワードを入力し、認証を受けることも可能である。なお、ここで行われるＩＤ要求以降の認証手順は、ＩＥＥＥ８０２．１ｘに記載されている手順であるので、本明細書では、その手順の説明を省略する。

【００８８】

そして、上位認証が確立されると、会議システム管理サーバ１０は、参加者端末の認証ルートを判定し、８０２．１ｘ認証を受けた接続であると判断すると（Ｓ７０）、認証のアカウントを確認し、正規アカウント保持者であれば、会議参加者権限に加え、他のネットワークアクセスまで許可するＩＰアドレスを割り当て、先に配布されているアカウントによる認証者の場合には、会議参加者に与えられるアクセス制限がかかるＩＰアドレスを、参加者端末に与える（Ｓ７１）。

【００８９】

ここで、仮に８０２．１ｘサプリカント機能を持たない端末が、上位認証を行う設定となっているアクセスポイント２０に接続した場合、無線リンク接続は、ＰＩＮコード入力なしに確立される。しかし、リンク確立後に、参加者端末では認証要求手順が行われないので、その後のアクセスを実行することができない。

【００９０】

一方、８０２．１ｘサプリカント機能を有する参加者端末が、リンクレベル認証が設定されているアクセスポイント２０に、リンク接続した場合、アクセスポ

イント２０から、リンク接続時に、ＰＩＮコード要求を受信する。そして、参加証によって通知されているＰＩＮコードによって、リンクレベル認証が確立されると、続いて、８０２．１ｘサプリカント機能によって、上位認証要求が参加者端末から発行される。

【００９１】

この信号を受信したアクセスポイント２０では、認証手順としてリンクレベル認証のみが有効となっているので、認証要求を無視する。そして、この参加者用に設定されたＰＩＮコードによる接続であると、会議システム管理サーバ１０が判断し、会議参加者に与えられるアクセス制限がかかるＩＰアドレスを、参加者端末に与える。

【００９２】

８０２．１ｘサプリカント機能を有する参加者端末が、リンクレベル認証を設定したアクセスポイント２０に接続した場合、８０２．１ｘ認証を行わない例について記載しているが、リンクレベル認証の場合でも、参加者端末から上位認証要求が発行されると、上位認証手順を行い、その認証アカウントに応じたＩＰアドレスの割り当てを行わせるようにしてもよい。

【００９３】

また、認証するプロトコルのレベルに応じて、アクセスポイント２０を変える例について説明したが、この構成に限定されることはなく、たとえば１つのアクセスポイント２０に、複数の通信チャネル（独立したピコネットを形成できる構成）を持たせることによって、上記と同様の動作を実現することができる。

【００９４】

また、本実施例では、上位認証機能を、会議システム管理サーバ１０に持たせるが、これに限定されることはなく、たとえば上位認証機能を、アクセスポイント２０内に持たせ、認証情報を、会議システム管理サーバ１０から取得できる手段を設けることによって、上記と同様の動作を行わせるようにしてもよい。

【００９５】

第３の実施例によれば、会議に参加する端末の認証を、複数のプロトコルレベルで行わせる手段を持たせるので、会議参加者の持ち込む端末の制限をなくすこ

とができ、また、上位認証を受けることができる機器においては、その認証機能の設定を、会議のためだけに変更することがなくなり、さらに、セキュリティレベルを保持したまま、リンクレベル認証に必要となるＰＩＮコード入力を省くことができ、煩雑な操作と設定とを行うことなく、会議に参加できる。

【００９６】

上記実施例によれば、電子メール等で予め配布される会議参加証に記載されてあるＰＩＮコードを用い、会議の参加者であるか主催者であるかを判別し、データのアクセス制限をかけるので、データの不正な改ざんを防ぐことができ、また、制限の設定を、アプリケーション上で別個に行う手間を省くことができる。

【００９７】

また、上位プロトコルによる認証手順に対応し、上位認証機能を有する端末については、ＰＩＮコード入力を省くので、セキュリティを確保しつつ、非対応の端末と同様の操作で、会議に参加することができる。

【００９８】

なお、上記実施例において、ＰＣ４０の代わりに、ＰＤＡを使用するようにしてもよい。

【００９９】

【発明の効果】

本発明によれば、会議システム等のネットワークに接続する機器によるデータの不正な改ざんや情報の漏洩を防ぐことができ、しかも、機能制限を、アプリケーション上で別個に行う手間を省くことことができるという効果を奏する。

【図面の簡単な説明】

【図１】

本発明の第１の実施例である無線通信システムＷＣ１のブロック図である。

【図２】

本実施例における会議システム管理サーバ１０を示すブロック図である。

【図３】

本実施例において、会議の主催者が会議に参加するまでの動作を示すフローチャートである。

【図４】

本実施例において、会議の参加者が会議に参加するまでの動作を示すフローチャートである。

【図５】

本実施例において、主催者がアクセスポイント２０のＰＩＮコードを変更する処理を示すシーケンス図である。

【図６】

本実施例において、参加者が会議に参加する場合の処理を示すシーケンス図である。

【図７】

本実施例において、主催者または参加者から送られた参加証を受信した際に、会議システム管理サーバの判別部１９の動作を示すフローチャートである。

【図８】

上記実施例において、会議システムによって制限される機能のテーブルを示す図である。

【図９】

本発明の第３の実施例における各無線端末の操作と、その操作に従った会議システム管理サーバ１０の動作を示すフローチャートである。

【符号の説明】

ＷＣ１…無線通信システム、

１０…会議システム管理サーバ、

２０…アクセスポイント、

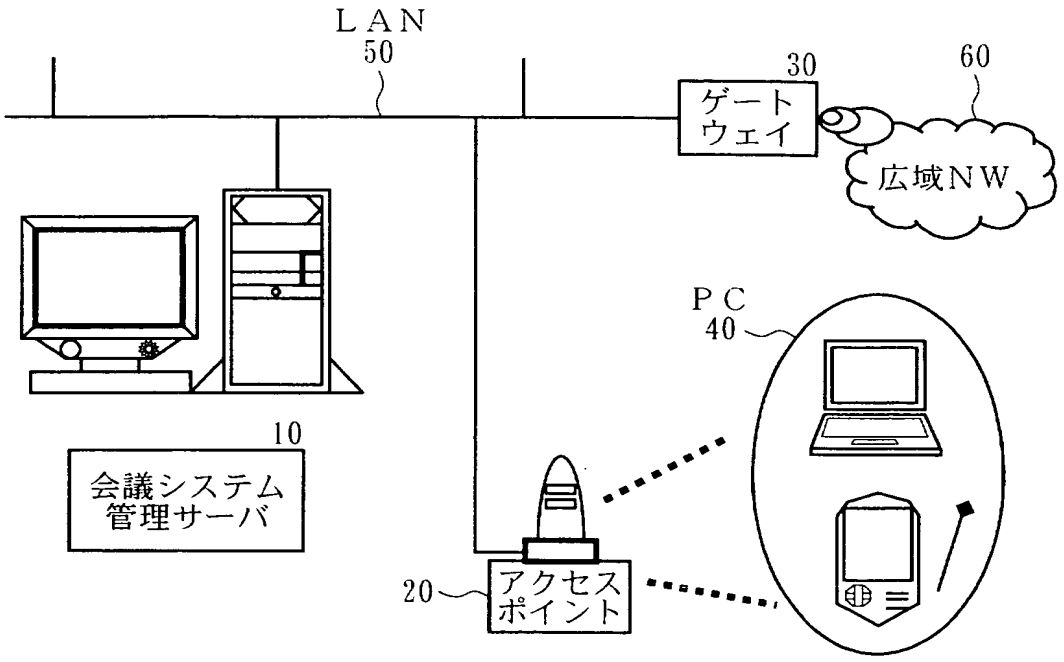
３０…ゲートウェイ、

４０…無線端末としてのＰＣ、

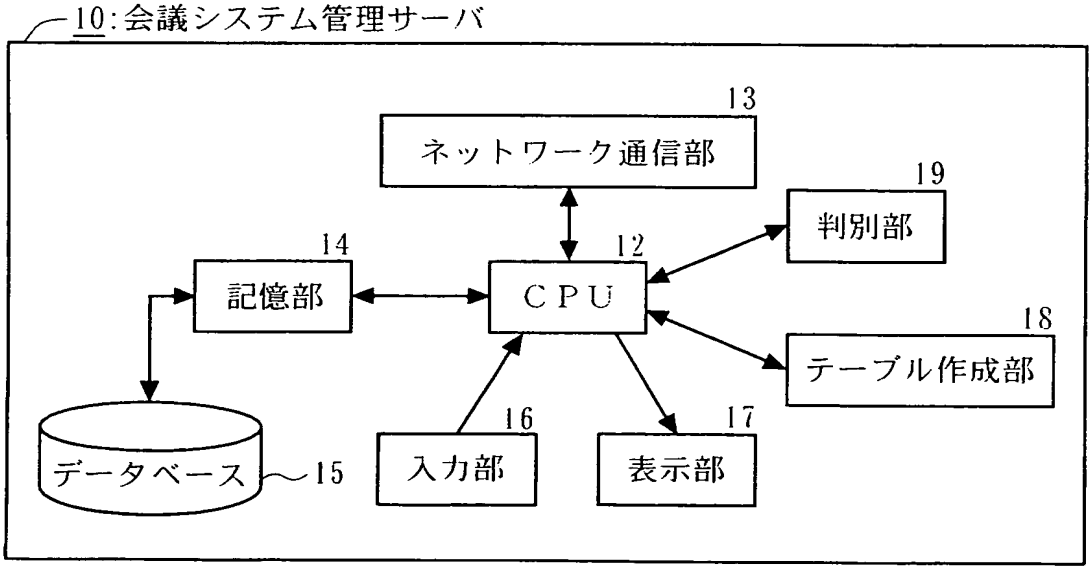
５０…ＬＡＮ。

【書類名】　図面

【図１】


WC１：無線通信システム
LAN
50
30
ゲート
ウェイ
60
広域NW
PC
40
10
会議システム
管理サーバ
20
アクセス
ポイント

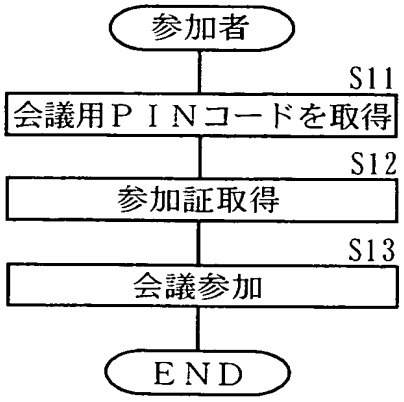
【図２】


10:会議システム管理サーバ
13
ネットワーク通信部
19
判別部
14
記憶部
12
CPU
18
テーブル作成部
データベース
15
16
入力部
17
表示部

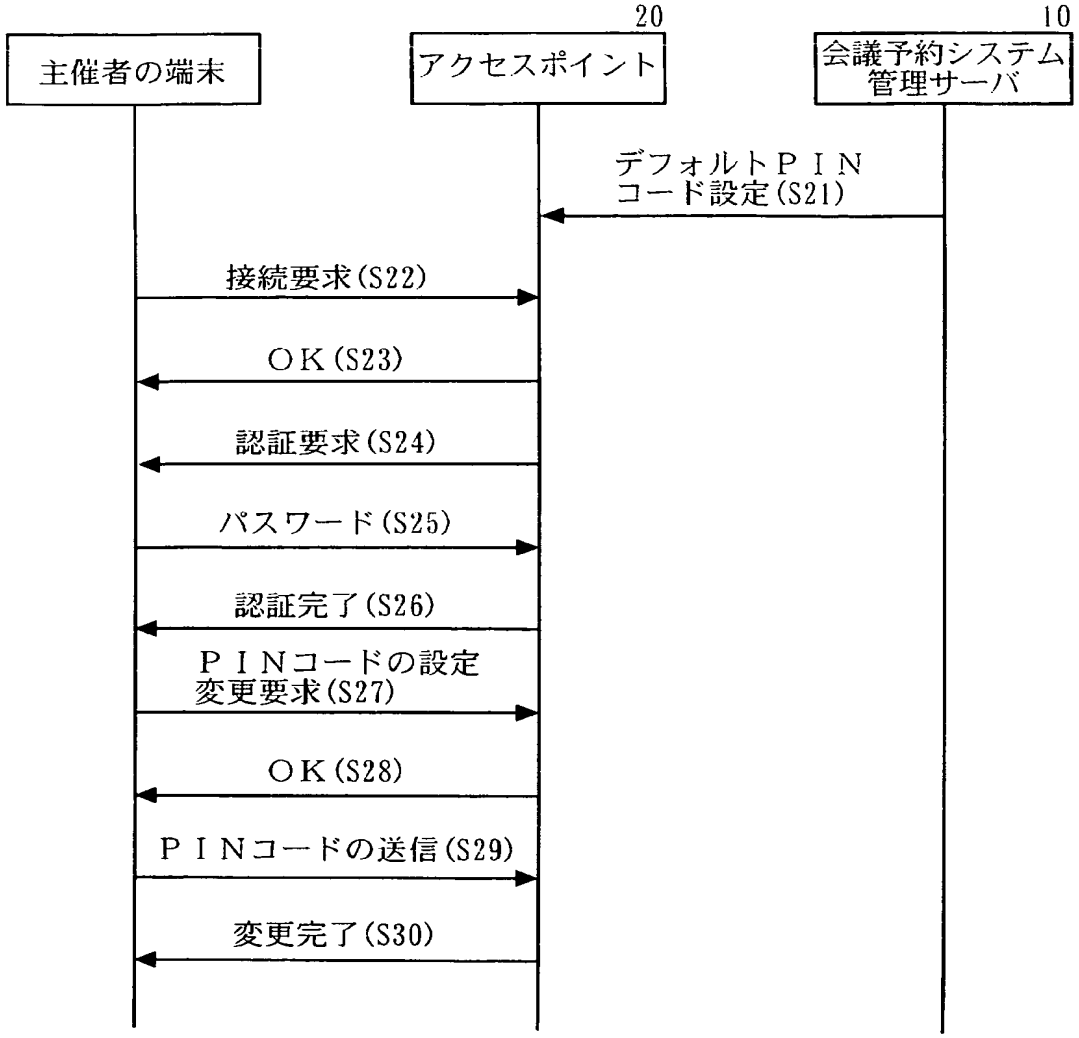
【図３】


主催者
S1
会議室予約
S2
ＰＩＮコードの設定変更
S3
変更したＰＩＮコードを参加者に通知
S4
参加証作成
S5
参加証配布
S6
会議参加
END

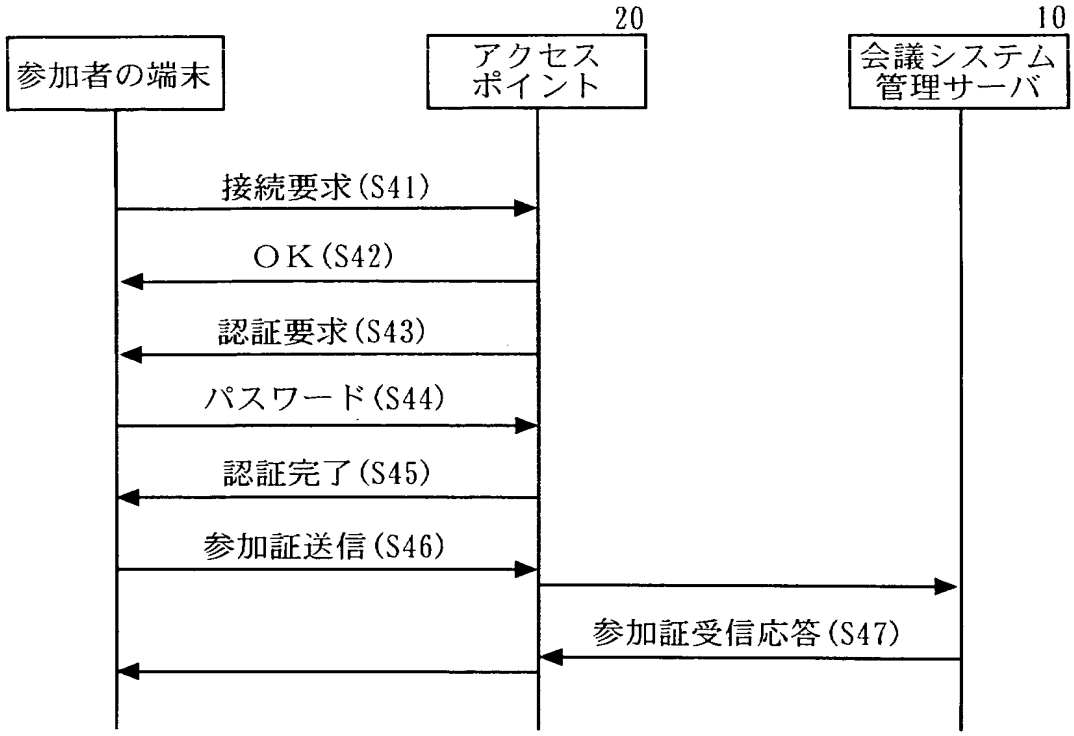
【図４】


参加者
S11
会議用ＰＩＮコードを取得
S12
参加証取得
S13
会議参加
END

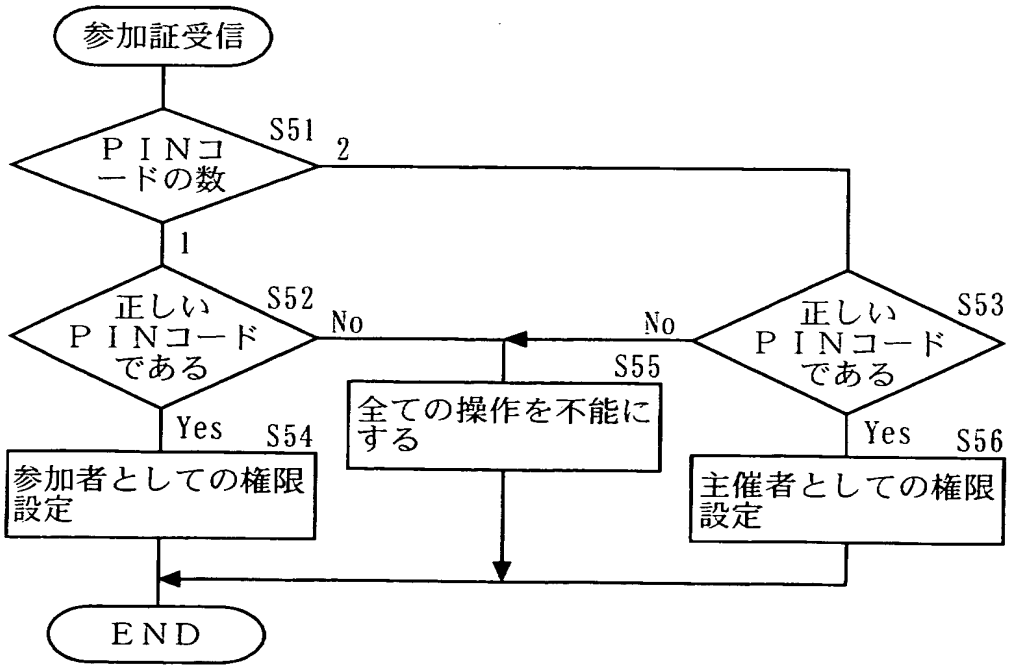
【図５】


主催者の端末
20
アクセスポイント
10
会議予約システム
管理サーバ
デフォルトＰＩＮ
コード設定(S21)
接続要求(S22)
ＯＫ(S23)
認証要求(S24)
パスワード(S25)
認証完了(S26)
ＰＩＮコードの設定
変更要求(S27)
ＯＫ(S28)
ＰＩＮコードの送信(S29)
変更完了(S30)

【図６】


参加者の端末
20
アクセス
ポイント
10
会議システム
管理サーバ
接続要求(S41)
ＯＫ(S42)
認証要求(S43)
パスワード(S44)
認証完了(S45)
参加証送信(S46)
参加証受信応答(S47)

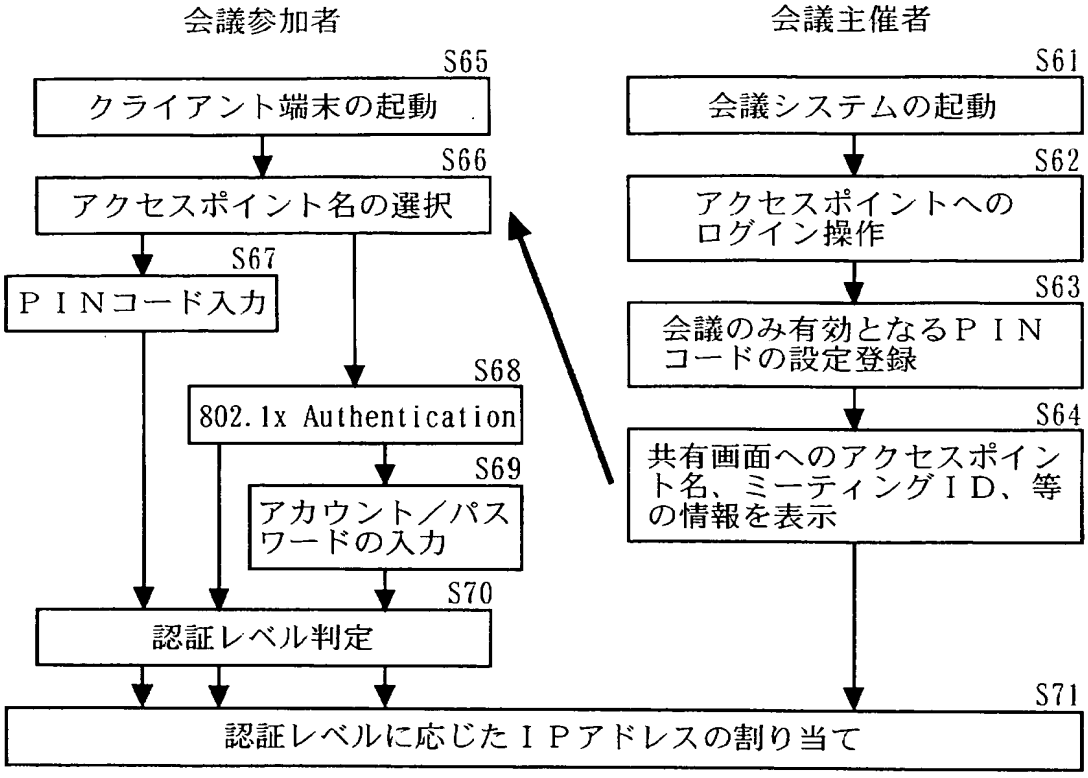
【図７】


参加証受信
ＰＩＮコードの数
S51
2
1
正しいＰＩＮコードである
S52
No
No
正しいＰＩＮコードである
S53
S55
全ての操作を不能にする
Yes
S54
参加者としての権限設定
Yes
S56
主催者としての権限設定
END

【図８】

機能	主催者	参加者
ファイルの閲覧	○	○
ファイルコピー	○	×
ファイル削除	○	×
ファイル印刷	○	×
ファイル名変更	○	×
ファイル上書き	○	×
ファイル保存	○	×
ネット閲覧	○	△
ＩＰアドレスの変更	○	×
ＰＩＮコードの変更	○	×
メール送受信	○	×

【図９】


会議参加者
会議主催者
S65
クライアント端末の起動
S66
アクセスポイント名の選択
S67
ＰＩＮコード入力
S68
802.1x Authentication
S69
アカウント／パスワードの入力
S70
認証レベル判定
S61
会議システムの起動
S62
アクセスポイントへのログイン操作
S63
会議のみ有効となるＰＩＮコードの設定登録
S64
共有画面へのアクセスポイント名、ミーティングＩＤ、等の情報を表示
S71
認証レベルに応じたＩＰアドレスの割り当て

【書類名】　　要約書

【要約】

【課題】　会議システム等のシステムに接続する機器によるデータの不正な改ざんや情報の漏洩を防ぐことができ、しかも、機能制限をアプリケーション上で別個に行う手間を省くことができる通信システムのサーバ装置を提供することを目的とするものである。

【解決手段】　会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、認証手続きを行う際に用いる認証情報に基づいて、上記参加者の立場を判別する参加者判別手段を有することを特徴とするサーバ装置である。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－１８９９２４
受付番号	５０３０１１００３２４
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　７月　７日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000001007
【住所又は居所】	東京都大田区下丸子３丁目３０番２号
【氏名又は名称】	キヤノン株式会社

【代理人】　申請人

【識別番号】	100087446
【住所又は居所】	東京都新宿区四谷２丁目４番１２号　大久保ビル６階
【氏名又は名称】	川久保　新一

特願２００３－１８９９２４

出　願　人　履　歴　情　報

識別番号　　［０００００１００７］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社